(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－23420
（P2003－23420A）
(43)公開日　平成15年１月24日(2003.1.24)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ	13/00	３５３Ｃ　５Ｂ０８５
Ｇ０６Ｆ	13/00	３５３		15/00	３１０Ｅ　５Ｂ０８９
	15/00	３１０	Ｇ０９Ｃ	1/00	６４０Ｅ　５Ｊ１０４
Ｇ０９Ｃ	1/00	６４０			６６０Ｅ　５Ｋ０３０
		６６０	Ｈ０４Ｌ	12/56	Ａ　５Ｋ０６７

審査請求　有　請求項の数35　ＯＬ　（全 18 頁）　最終頁に続く

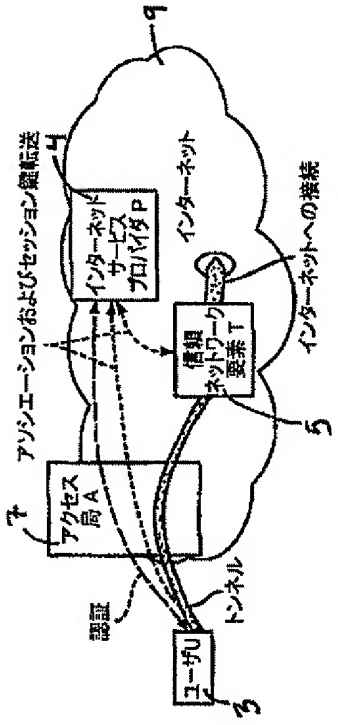
(21)出願番号　特願2002－69405(P2002－69405)
(22)出願日　平成14年３月14日(2002.3.14)
(31)優先権主張番号　６０／２７８４３６
(32)優先日　平成13年３月26日(2001.3.26)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　１０／０５７９１４
(32)優先日　平成14年１月29日(2002.1.29)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　イェンスーピーター　レドリッヒ
アメリカ合衆国，ニュージャージー　08540　プリンストン，４　インディペンデンス　ウエイ，エヌ・イー・シー・ユー・エス・エー　インク内
(74)代理人　100097157
弁理士　桂木　雄二

最終頁に続く

(54)【発明の名称】　信頼されないアクセス局を介した通信方法

(57)【要約】
【課題】　公衆インターネットやプライベートＬＡＮのようなパブリックまたはプライベートＩＰネットワークへのアクセスのために、既存のインフラストラクチャの共有を可能にするメカニズムを提供する。
【解決手段】　端末Ｕと非信頼アクセス局Ａの間に接続を確立する。次に、端末Ｕと契約しているインターネットサービスプロバイダ（ＩＳＰ）ＰへＩＳＰ認証要求を送信する。ＩＳＰ　Ｐと端末Ｕが正しく認証された後、端末Ｕと信頼ゲートウェイＴの間に信頼された接続を確立する。こうして確立される安全なトンネルにより、ＩＳＰ　Ｐは、端末Ｕに所定のサービスを提供するために、アクセス局Ａにおけるリソースの制御を動的に取得することが可能となる。端末ＵとＩＳＰ　Ｐの正当な認証後、ＩＳＰ　Ｐは、データパケットを暗号化するためのセッション鍵を生成することも可能である。



【特許請求の範囲】
【請求項１】　ユーザの端末（Ｕ）とインターネットへの信頼ゲートウェイ（Ｔ）との間で非信頼アクセス局（Ａ）を介して安全な通信を確立する通信方法において、
端末（Ｕ）と非信頼アクセス局（Ａ）の間のアソシエーションを確立するステップと、
端末（Ｕ）からＩＳＰ（Ｐ）へ前記非信頼アクセス局（Ａ）を介してＩＳＰ認証パケットを送信するステップと、
前記ＩＳＰ（Ｐ）から前記端末（Ｕ）へ前記非信頼アクセス局（Ａ）を介してユーザ認証パケットを送信するステップと、
前記ＩＳＰにおいて、
前記端末（Ｕ）と前記ＩＳＰ（Ｐ）との認証後、前記端末（Ｕ）と信頼ゲートウェイ（Ｔ）との間のトラフィックを暗号化するために使用されるセッション鍵を生成するステップと、
前記セッション鍵を前記端末（Ｕ）および前記信頼ゲートウェイ（Ｔ）に配送するステップと、
前記端末（Ｕ）が前記信頼ゲートウェイ（Ｔ）を介してインターネットと通信することができるような安全なトンネルを確立するステップと、
を有し、
前記安全なトンネルは、前記端末（Ｕ）と前記インターネットの間で前記信頼ゲートウェイ（Ｔ）を介して送信されるトラフィックが、第三者の前記非信頼アクセス局（Ａ）による変更または傍受から安全であるように、前記端末（Ｕ）と前記信頼ゲートウェイ（Ｔ）の間の物理リンクをエミュレートする、
ことを特徴とする通信方法。
【請求項２】　前記ＩＳＰ認証パケットは、前記ＩＳＰ（Ｐ）の身元を認証するための、前記端末（Ｕ）から前記ＩＳＰ（Ｐ）への認証チャレンジ（ＣＨ＿Ｕ）を含むことを特徴とする請求項１記載の方法。
【請求項３】　前記ユーザ認証パケットは、前記端末（Ｕ）のユーザの身元を認証するための、前記ＩＳＰ（Ｐ）から前記端末（Ｕ）への認証チャレンジ（ＣＨ＿Ｐ）を含むことを特徴とする請求項１記載の方法。
【請求項４】　非信頼アクセスポイントを有する非信頼インフラストラクチャを介してＩＰベースのネットワークへのパブリックアクセスを提供する方法において、
ＩＰ装置（Ｕ）と前記非信頼アクセスポイント（Ａ）の間に、ＩＰアドレスが該ＩＰ装置に動的に割り当てられる接続を確立するステップと、
ＩＳＰ認証要求を、前記ＩＰ装置（Ｕ）から、前記ＩＰ装置（Ｕ）が契約しているインターネットサービスプロバイダ（ＩＳＰ）（Ｐ）へ、第三者所有の前記非信頼インフラストラクチャに所属する前記非信頼アクセスポイント（Ａ）を通じて、送信するステップと、
前記ＩＰ装置（Ｕ）が前記ＩＳＰ（Ｐ）と契約している正当なユーザであるかどうかを判断するためのユーザ認証要求を、前記ＩＳＰ（Ｐ）から、前記ＩＰ装置（Ｕ）へ、前記第三者所有の非信頼インフラストラクチャに所属する前記非信頼アクセスポイント（Ａ）を通じて、送信するステップと、
前記ＩＳＰ（Ｐ）において、
前記ＩＳＰ認証要求および前記ユーザ認証要求が正当であるとき、前記ＩＰ装置（Ｕ）と信頼ノード（Ｔ）の間で送信されるデータを暗号化するために使用される、データパケットを暗号化するためのセッション鍵を生成するステップと、
前記セッション鍵を前記ＩＰ装置（Ｕ）および前記信頼ノード（Ｔ）に配送するステップと、
を有し、さらに、
前記ＩＰ装置（Ｕ）とインターネットの間で非信頼アクセスポイント（Ａ）を介して送信されるデータパケットが、安全なトンネルにおいて、前記非信頼アクセスポイント（Ａ）による変更および操作から保護されるように、前記ＩＰ装置（Ｕ）と前記信頼ノード（Ｔ）の間で送信されるデータパケットを暗号化するために前記セッション鍵が使用される安全なトンネルを確立するステップを有することを特徴とする、ＩＰベースのネットワークへのパブリックアクセスを提供する方法。
【請求項５】　非信頼アクセス局（Ａ）を有する第三者所有の非信頼インフラストラクチャを通じてＩＰベースのネットワークへのパブリックアクセスを提供する方法において、
ＩＰ装置（Ｕ）と前記アクセス局（Ａ）の間に、ＩＰアドレスが該ＩＰ装置に動的に割り当てられる接続を確立するステップと、
前記ＩＰ装置（Ｕ）が契約しているインターネットサービスプロバイダ（ＩＳＰ）（Ｐ）へ、該ＩＳＰ（Ｐ）が真正であることの証明を要求するＩＳＰ認証要求を送信するステップと、
前記ＩＳＰ（Ｐ）から前記ＩＰ装置（Ｕ）へ、前記ＩＰ装置（Ｕ）が前記ＩＳＰ（Ｐ）とサービス契約を結んでいるかどうかを確認するためのユーザ認証要求を送信するステップと、
前記ＩＳＰ（Ｐ）および前記ＩＰ装置（Ｕ）が正しく認証された後、前記ＩＰ装置（Ｕ）と信頼ゲートウェイ（Ｔ）との間に信頼された接続を確立するステップと、
を有し、
前記信頼された接続を通して、前記ＩＳＰ（Ｐ）は、前記ＩＰ装置（Ｕ）に所定のサービスを提供するために、前記非信頼アクセス局（Ａ）におけるリソースの制御を動的に取得可能であることを特徴とする、ＩＰベースのネットワークへのパブリックアクセスを提供する方法。
【請求項６】　端末（Ｕ）と、該端末と契約しているインターネットサービスプロバイダ（Ｐ）と、インターネ

ットとの間に、第三者所有の非信頼アクセス局（Ａ）を通じて安全な接続を確立する方法において、
前記端末（Ｕ）と前記アクセス局（Ａ）との間に接続を確立するステップと、前記端末（Ｕ）および前記インターネットサービスプロバイダ（ＩＳＰ）（Ｐ）へＩＳＰ認証要求を送信するステップと、
前記ＩＳＰ（Ｐ）および前記端末（Ｕ）が正しく認証された後、前記端末（Ｕ）と信頼ノード（Ｔ）との間に信頼された接続を確立するステップと、
を有し、
前記信頼された接続により、前記ＩＳＰ（Ｐ）は、前記端末（Ｕ）に所定のサービスを提供するために、前記非信頼アクセス局（Ａ）におけるリソースの制御を動的に取得可能であることを特徴とする、非信頼アクセス局を通じて安全な接続を確立する方法。

【請求項７】　前記ＩＳＰ認証要求は、前記ＩＳＰ（Ｐ）の身元を認証するための、前記端末（Ｕ）から前記ＩＳＰ（Ｐ）への認証チャレンジ（ＣＨ＿Ｕ）を含むことを特徴とする請求項６記載の方法。

【請求項８】　前記ユーザ認証要求は、前記端末（Ｕ）が前記ＩＳＰ（Ｐ）のサービスに加入しているという身元を認証するための、前記ＩＳＰ（Ｐ）から前記端末（Ｕ）への認証チャレンジ（ＣＨ＿Ｐ）を含むことを特徴とする請求項６記載の方法。

【請求項９】　前記端末（Ｕ）および前記ＩＳＰ（Ｐ）の正当な認証後、前記ＩＳＰ（Ｐ）は、データパケットを暗号化するためのセッション鍵を生成することを特徴とする請求項６記載の方法。

【請求項１０】　前記ＩＳＰ（Ｐ）は、前記インターネットの前記信頼ノード（Ｔ）を選択することを特徴とする請求項６記載の方法。

【請求項１１】　前記ＩＳＰ（Ｐ）は、前記端末（Ｕ）および前記信頼ノード（Ｔ）に前記セッション鍵を配送することを特徴とする請求項９記載の方法。

【請求項１２】　セッション鍵が、前記端末（Ｕ）と前記信頼ノード（Ｔ）との間で送信されるデータパケットを暗号化するために使用されることを特徴とする請求項６記載の方法。

【請求項１３】　前記端末（Ｕ）と前記信頼ノード（Ｔ）との間での暗号化されたデータパケットの送信により安全なトンネルを確立することを特徴とする請求項１２記載の方法。

【請求項１４】　前記安全なトンネルは、前記非信頼アクセス局による操作からデータパケットを保護することを特徴とする請求項１３記載の方法。

【請求項１５】　前記信頼された接続の確立後、タイムアウト値が信頼ノード（Ｔ）および端末（Ｕ）に配送されることを特徴とする請求項６記載の方法。

【請求項１６】　前記タイムアウト値は所定の期間に設定され、前記信頼された接続は、前記タイムアウト値に等しい期間のあいだ有効であり、タイムアウト時には前記信頼された接続のために利用されたリソースが解放される、ことを特徴とする請求項１５記載の方法。

【請求項１７】　前記信頼ノード（Ｔ）は、前記端末（Ｕ）から暗号化されたデータパケットを受信した後、該データパケットを復号し、復号されたデータパケットをインターネットに転送することを特徴とする請求項６記載の方法。

【請求項１８】　前記信頼ノード（Ｔ）は、前記端末（Ｕ）から暗号化されたデータパケットを受信した後、該データパケットを復号し、復号されたデータパケットをリモート通信相手（Ｒ）に転送することを特徴とする請求項１７記載の方法。

【請求項１９】　前記インターネットは、前記信頼ノード（Ｔ）を介して前記端末（Ｕ）へもとのデータパケットを送信し、前記信頼ノード（Ｔ）は、もとのデータパケットを暗号化し、暗号化されたデータパケットを、前記非信頼アクセス局（Ａ）を介して前記端末（Ｕ）に転送することを特徴とする請求項１８記載の方法。

【請求項２０】　前記端末（Ｕ）は、前記信頼ノード（Ｔ）から暗号化されたデータパケットを受信した後、セッション鍵を利用して該データパケットを復号することにより、インターネットからのもとのデータパケットを得ることを特徴とする請求項１７記載の方法。

【請求項２１】　前記リモート通信相手（Ｒ）が、前記信頼ノード（Ｔ）を介して前記端末（Ｕ）へもとのデータパケットを送信し、前記信頼ノード（Ｔ）は、もとのデータパケットを暗号化し、暗号化されたデータパケットを、前記非信頼アクセス局（Ａ）を介して前記端末（Ｕ）に転送することを特徴とする請求項１８記載の方法。

【請求項２２】　前記端末（Ｕ）は、前記信頼ノード（Ｔ）から暗号化されたデータパケットを受信した後、セッション鍵を利用して該データパケットを復号することにより、前記リモート通信相手（Ｒ）からのもとのデータパケットを得ることを特徴とする請求項２１記載の方法。

【請求項２３】　前記ＩＳＰ（Ｐ）は、前記端末（Ｕ）によって利用されたリソースについて、前記非信頼アクセス局（Ａ）に時間のアカウンティングを提供することを特徴とする請求項６記載の方法。

【請求項２４】　前記非信頼アクセス局（Ａ）は、第三者所有のネットワークインフラストラクチャに組み込まれていることを特徴とする請求項６記載の方法。

【請求項２５】　前記ＩＳＰ（Ｐ）は、前記非信頼アクセス局（Ａ）を介して、少なくとも１つの加入サービスを前記端末（Ｕ）に提供することを特徴とする請求項２４記載の方法。

【請求項２６】　前記ＩＳＰ（Ｐ）は、時間のアカウンティングに従って、前記端末（Ｕ）に対して費やされた

リソースについて、前記非信頼アクセス局（Ａ）に償還することを特徴とする請求項６記載の方法。
【請求項２７】　前記ＩＳＰ（Ｐ）は、前記端末（Ｕ）に提供されたサービスについて当該端末（Ｕ）に課金することを特徴とする請求項２５記載の方法。
【請求項２８】　前記非信頼アクセス局（Ａ）は、公共施設のネットワークインフラストラクチャ内に位置することを特徴とする請求項２４記載の方法。
【請求項２９】　前記公共施設は、空港、会議場、レストラン、ホテル、図書館、および学校のうちの少なくとも１つであることを特徴とする請求項２８記載の方法。
【請求項３０】　前記非信頼アクセス局（Ａ）は、私宅のインフラストラクチャ内に、または、企業もしくは政府機関の私設インフラストラクチャ内に位置することを特徴とする請求項２４記載の方法。
【請求項３１】　前記非信頼アクセス局（Ａ）は、ＷＬＡＮ（ＩＥＥＥ８０２．１１）、Ｂｌｕｅｔｏｏｔｈ（ＩＥＥＥ８０２．１５）、またはＨｉｐｅｒＬａｎを含む少なくとも１つのワイヤレス伝送標準と互換であることを特徴とする請求項６記載の方法。
【請求項３２】　前記端末（Ｕ）はモバイル装置であることを特徴とする請求項６記載の方法。
【請求項３３】　前記端末（Ｕ）は、動的ホスト設定プロトコル（ＤＨＣＰ）要求をブロードキャストし、前記非信頼アクセス局（Ａ）から「マジック」ＤＨＣＰ応答を受信することによって、互換アクセスポイントを認識することを特徴とする請求項６記載の方法。
【請求項３４】　前記非信頼アクセス局（Ａ）は、同時に複数の端末（Ｕ）にサービスするときには、端末とデータパケットとのマッチングを容易にするために、ローカル固有識別（ＬＵＩＤ）を端末（Ｕ）に割り当てることを特徴とする請求項６記載の方法。
【請求項３５】　非信頼アクセスポイントを介してインターネットサービスのアクセスおよび認証を行うコンピュータプログラム製品において、
コンピュータに所定の動作を実行させるソフトウェア命令と、
前記ソフトウェア命令を保持するコンピュータ可読媒体と、を有し、
前記所定の動作は、
ＩＰ装置（Ｕ）とアクセス局（Ａ）の間に、ＩＰアドレスが該ＩＰ装置（Ｕ）に動的に割り当てられる接続を確立するステップと、
前記ＩＰ装置（Ｕ）が契約しているインターネットサービスプロバイダ（ＩＳＰ）（Ｐ）へ、該ＩＳＰ（Ｐ）が真正であることの証明を要求するＩＳＰ認証要求を送信するステップと、
前記ＩＳＰ（Ｐ）から前記ＩＰ装置（Ｕ）へ、前記ＩＰ装置（Ｕ）が前記ＩＳＰ（Ｐ）とサービス契約を結んでいるかどうかを確認するためのユーザ認証要求を送信するステップと、
前記ＩＳＰ（Ｐ）および前記ＩＰ装置（Ｕ）が正しく認証された後、前記ＩＰ装置（Ｕ）と信頼ゲートウェイ（Ｔ）の間に信頼された接続を確立するステップとを含み、
前記信頼された接続により、前記ＩＳＰ（Ｐ）は、前記ＩＰ装置（Ｕ）に所定のサービスを提供するために、信頼されない第三者所有の前記アクセス局（Ａ）におけるリソースの制御を動的に取得可能であることを特徴とする、非信頼アクセスポイントを介してインターネットサービスのアクセスおよび認証を行うコンピュータプログラム製品。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はＩＰネットワークへのパブリックアクセスを提供するシステムに係り、特に、第三者所有の信頼されない（非信頼）アクセスノードを通じて、インターネットサービスプロバイダがその加入者にインターネットアクセスを提供する際の通信方法に関する。
【０００２】
【従来の技術】下記の文献は、ワイヤレス技術に関する有用な背景的知識を提供する。
【０００３】1) Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, John Wiley &; Sons, 1995, ISBN 0471170 99.
【０００４】2) R. Droms, "Dynamic Host Configuration Protocol (DHCP)", IETF RFC 2131, 1997.
【０００５】3) Egevang, K. and Francis, P., "The IP Network Address Translator (NAT), IETF RFC 1631, 1994.
【０００６】本発明は、第三者が運営するアクセス局を用いて、公衆インターネット、社内イントラネット、あるいはプライベートＬＡＮのようなＩＰネットワークへのパブリックアクセスを提供するシステムおよび方法において、ユーザも、このユーザのＩＳＰも、いずれもそのアクセス局の正確なオペレーションを信頼していないため、そのアクセス局が「非信頼」アクセス局となっているような場合のシステムおよび方法に関する。より具体的には、本発明は、悪意のある可能性があり、それゆえ信頼されない（非信頼）第三者によって運営されるアクセス局を介してＩＰネットワークにアクセスするために、データの認証(authentication)、権限付与(authorization)、アカウンティング(accounting)、および暗号化を実行する方法に関する。本発明の方法およびシステムは、ワイヤレス（無線）およびワイヤライン（有線）のアクセスに関して同様に使用可能である。ここで、「ワイヤレス」とは、無免許周波数帯で動作する短距離技術であることも、より長距離の免許を受けた電波技術

であることも可能である。

【０００７】インターネットのようなＩＰネットワークへの従来技術のパブリックアクセスは、インターネットサービスプロバイダ（ＩＳＰ）を通じて提供されている。ＩＳＰは、モデムのような伝送設備も所有またはリースする。ほとんどの場合、インターネットにアクセスしたいユーザは、与えられた地域エリアのＩＳＰとサービス契約を締結しなければならない。移動する加入者にサービス範囲を拡大するため、一部のＩＳＰは、認証、権限付与およびアカウンティングの手続きを管理するローミング契約を結んでいる。同様の手続きは、セルラ事業者についても行われ、与えられた事業者の加入者が別の事業者のカバレジエリアに移動することを可能にしている。しかし、これらの確立された手続きは、ネットワークアクセスが信頼できることを仮定している。この仮定は、ダイヤルアップモデムバンクのようなプライベートアクセスメカニズム、インフラストラクチャの高いコスト、および、セルラ事業者の場合の周波数スペクトルの排他的所有によって保証されていた。

【０００８】無免許周波数スペクトルで運営される安価なインフラストラクチャを用いてＩＰネットワークへのワイヤレスアクセスを可能にする第２の従来技術の出現は、小規模の独立系アクセスプロバイダの新設を容易にしている。ワイヤレスローカルエリアネットワーク（ＷＬＡＮ）およびパーソナルエリアネットワーク（ＰＡＮ）に基づくそれらのワイヤレスアクセス技術の到達範囲は小さいため、与えられた地所における公衆インターネットアクセスのためのインフラストラクチャの運営は、その地所の所有者によって管理される。実際、ケーブルやＤＳＬを通じての高速インターネットアクセスを有するアパートや家屋の所有者であれば、ＷＬＡＮアクセスポイントを運営することによって、近隣にアクセスを提供することができる。しかし、そのようなワイヤレスアクセスポイントへのアクセスは、同じ組織あるいは家庭の装置に制限される。外来のＩＰ装置（例えば、自分のＷＬＡＮカードを装備した訪問者や、ＷＬＡＮカードを装備したＰＣを持っている隣人）にアクセスを提供することは安全（セキュア）でなく、通常は許可されず、技術的に不可能なこともある。さらに、私有のアクセス局は通常、その所有者のＩＳＰに接続されている。すなわち、別のＩＳＰに加入したゲストは、自分のＩＳＰによって提供されるサービスを取得することができず、インターネットアクセスのために自分のＩＳＰによって課金されることもできない。

【０００９】

【発明が解決しようとする課題】上記第１の従来技術として説明したパブリックアクセスを可能にするメカニズムを、上記第２の従来技術として説明した小さい地理的エリアにおけるインターネットアクセスを提供する小規模独立系事業者に適用することは、さまざまな問題点および欠点を有する。例えば、ローミングユーザは、ＷＬＡＮの事業者の信頼性を知らない。悪意のある事業者が、ユーザとコンテンツプロバイダの間の通信を傍受するのが容易であることを発見するかもしれない。そのような事業者は、ユーザのトラフィックからログイン名やパスワードのような資格証明を取得する手段を見つける可能性もある。さらに、従来技術の認証および権限付与の手続きでは、使用量に基づくアカウンティングが容易でない。これは、ローミングユーザに提供されるアクセスについての独立系事業者の精算のために必要となる。

【００１０】今日、私有のアクセス局は至る所で利用可能であり、インターネットにアクセスする潜在的手段をどこにいるユーザにも提供している。しかし、現在のＩＳＰは、自分でインフラストラクチャを構築しなければならず、これは、一時的ユーザをサポートすることに関しては高価であり、しばしば融通性に欠ける。

【００１１】本発明の目的は、第三者所有の信頼されない（非信頼）アクセスノードを通じて、インターネットサービスプロバイダがその加入者にインターネットアクセスを提供する安全な方法を提供することである。

【００１２】本発明のもう１つの目的は、インターネットサービスプロバイダとアクセスノード所有者の間、および、インターネットサービスプロバイダと加入者との間で、アカウンティング情報を提供することである。このアカウンティング情報は、システムの動作の一体をなす部分として導出され、悪意のある操作から保護される。

【００１３】

【課題を解決するための手段】本発明は、ＩＰネットワークへのアクセス局に関する。具体的には、本発明は、そのサービスのユーザおよびこのユーザのＩＳＰ以外の当事者によって所有され運営される、ＩＰネットワークへのアクセス局に関する。さらに具体的には、本発明は、コンピュータなどのＩＰベースの装置に、例えばインターネットや社内イントラネットのようなＩＰネットワークへのアクセスを提供することができる装置に関する。この場合、アクセス局は、サービスを希望するＩＰ装置から、ユーザの識別とユーザのＩＳＰの識別とを取得する。アクセス局は、サービスを取得したいというユーザの希望についてユーザのＩＳＰに通知する。ユーザのＩＳＰは、ユーザが加入したサービスを提供するために、アクセス装置内のリソースの制御を動的に取得する。最後に、ＩＳＰは、そのリソースの使用量に対するアクセス局の支払いを手配し、ユーザ（その加入者）の課金を手配する。

【００１４】本発明は、インターネットサービスプロバイダでインターネットサービスに加入したエンドユーザ、アクセスノードあるいはインフラストラクチャの所有者、および、インターネットへの信頼されるゲートウェイ、ならびに、第三者所有のアクセスノードを通じて

インターネットサービスの加入者に匿名インターネットアクセス提供を行う方法を含む。具体的には、本発明は、加入者とインターネットサービスプロバイダとの相互認証の手続き、および、エンドユーザとインターネットへの信頼ゲートウェイとの間の安全なトンネルの確立に必要な鍵配送とを含む。本発明の方法は、サービス要求のステップと、インターネットサービスプロバイダ認証のステップと、加入者認証のステップと、一意的なセッション鍵を生成するステップと、セッション鍵を信頼されるネットワークノードおよび加入者に配送するステップと、前に配送されたセッション鍵を用いて第三者アクセスノードを通じて加入者と信頼されるネットワーク要素との間に確立される安全なトンネルを用いてデータ転送を行うステップとを含む。

【００１５】本発明の方法は、さらに、インターネットサービスプロバイダから加入者、アクセスノードおよび前記信頼されるネットワーク要素にタイムアウト値を配送するステップを含む。タイムアウト値は、前記加入者とインターネットサービスプロバイダの間の再認証手続きをトリガする。

【００１６】さらに、本発明の方法は、加入者および信頼されるネットワーク要素に配置される、トンネルに関するタイマと、前記アクセスノードに配置される別のタイマのうちの１つが満期になった場合に、トンネルを解放するステップを含む。

【００１７】さらに、成功した認証の数に基づいてアカウンティング情報を生成する方法が提供される。アカウンティング情報を用いてプリペイドサービスを提供し、再認証前の残り時間を判定する方法も提供される。

【００１８】本発明の応用分野としては以下の場合があるが、もちろん、これらに限定されるものではない。

・個人の家庭内のアクセス局が、ＷＬＡＮ（ＩＥＥＥ８０２．１１）、Ｂｌｕｅｔｏｏｔｈ（ＩＥＥＥ８０２．１５）、あるいはＨｉｐｅｒＬＡＮに基づくワイヤレスアクセスを訪問者や近隣に提供する場合。

・ホテルや空港が、その顧客のＩＳＰによって管理されるインターネットアクセスを顧客に提供するために、アクセス局（ＷＬＡＮ、Ｂｌｕｅｔｏｏｔｈ、ＨｉｐｅｒＬＡＮ）を所有し運営する場合。

・会議が、会議参加者に、その会議参加者のＩＳＰによって管理されるインターネットアクセスを与えるために、会議開催地でアクセス局（ＷＬＡＮ、Ｂｌｕｅｔｏｏｔｈ、ＨｉｐｅｒＬＡＮ）をリースし一時的に配備する場合。

【００１９】理解されるべき点であるが、明細書全体を通じて、「インターネット」という用語は、その最広義における「ＩＰに基づくネットワーク」を意味し、これには、公衆インターネット、社内イントラネット、プライベートまたはパブリック（公衆）ＬＡＮ、およびＩＰベースのアドホックネットワークが含まれるが、これらには限定されない。

【００２０】

【発明の実施の形態】以下、本発明の好ましい実施例について、図面を参照して説明する。

【００２１】以下の詳細な説明は、次のように構成される。「コンポーネントの概観」と題するセクションでは、システムのコンポーネントを紹介し、コンポーネントの相互関係の説明を行う。「本発明の動作」と題するセクションでは、本発明のさまざまな実施例と、その応用について説明する。さらに、理解と明確さを促進するために、本発明の説明は、「ＵとＰの相互認証」、「アクセス局Ａ（７）を通じての端末Ｕ（３）と信頼ノードＴ（５）の間の安全なトンネル（１）の作成」、「端末ＵとＩＰネットワークの間のデータ転送」、「トンネル解放とタイムアウト」、「課金」の各セクションに分けられる。

【００２２】［コンポーネントの概観］再度注意を喚起しておくが、「ＩＰネットワーク」という用語は、公衆インターネットおよび社内イントラネットを含む、すべての可能なＩＰベースのインフラストラクチャネットワークを表すために用いられる。

【００２３】ユーザの端末装置（Ｕ）

Ｕは、ユーザのＩＰベースの端末装置を表す。これは、インターネットプロトコルスイート（ＩＰ）を用いて他の装置と通信する移動式あるいは固定式の装置である。これには、ワークステーションコンピュータ、パーソナルコンピュータ（ＰＣ）、ラップトップコンピュータ、ハンドヘルドＰＣ、電話機あるいはその他のＩＰベースの装置あるいは機器が含まれるが、これらには限定されない。しかし、予想されるように、ほとんどの場合、この端末装置は、小型で移動式のものであり、ＩＰネットワークに接続するための有線またはワイヤレスの一方または両方の手段を有することになる（下記の「アクセス局」参照）。さらに、与えられた任意の時刻において、この装置は、高々１ユーザに関連づけられる、すなわち、「このユーザの装置」として認識できることが仮定される。

【００２４】アクセス局（Ａ）

Ａは、アクセス局を表す。アクセス局は、端末装置ＵをＩＰベースのインフラストラクチャネットワーク（例えば、イントラネットやインターネット）に接続するために使用される。アクセス局は、ＩＰネットワークからトラフィックを受け取り、それを正しい端末Ｕに配信するとともに、端末Ｕからトラフィックを受け取り、それをＩＰネットワークに転送する。ＡとＵの間の通信の手段は、有線でも無線でもよい。本発明は、両方の場合に適用がある。さらに、Ａは、所有者および運営者を有するとともに、例えば、ある周波数スペクトルを使用する許可を必要とする無線基地局（ベースステーション）の場合には、運営特権の所有者を有する。本明細書の目的の

ために、これらのすべての側面をＡという抽象概念にまとめる。

【００２５】通常、アクセス局Ａは、ＩＰネットワークに常時接続されるが、アクセス局Ａと端末Ｕの間の接続は本来一時的である。例えば、アクセス局Ａは、公共エリア（例えば、ホテル、空港、レストラン）に配置されることも、非公共エリア（例えば、個人の家庭内）に配置されることも可能である。後者の場合、アクセスは、物理的にアクセス可能なユーザ（例えば、Ａの所有者の訪問客）に制限されてもよく、あるいは、アクセスは、Ａの通信範囲内のすべてのユーザに利用可能であるとしてもよい（例えば、Ａは、Ａの近隣および訪問者にインターネットアクセスを提供するために利用可能な、私宅内の８０２．１１／Ｂｌｕｅｔｏｏｔｈ／ＨｉｐｅｒＬａｎ基地局である）。

【００２６】インターネットサービスプロバイダ（Ｐ）

Ｐは、インターネットサービスプロバイダ（ＩＳＰ）を表す。ＩＳＰは、サービスパラメータを規定するＵとＰの間の加入契約に基づいて、サービスを端末装置Ｕに提供する。このため、Ｐは、エンドユーザサービスについてＵに課金する責任があると仮定することができる。また、Ｐは、Ａのリソースを使用することについて、Ａに支払いをしなければならないと仮定することもできる。また、Ｕとその通信相手との間のトラフィックが、Ａからのパケットのスヌーピング／挿入／変更あるいはその他の攻撃に対して安全であることを保証することも、Ｐの責任である。

【００２７】通常、Ｐは、収益をあげるために、個人あるいは他の会社にインターネットアクセスおよびその他の関連サービス（例えば、電子メール）を提供する会社である。もう１つの可能性として、Ｐは、その従業員にＩＰネットワーク（例えば、社内イントラネット、公衆インターネット、あるいはプライベートＩＰネットワーク）へのアクセスを提供する会社である。ここでは、主要な目標は、直接的に収益をあげることではなく、従業員の作業プロセスのサポートである。例えば、ＦｅｄＥｘの従業員は、時折社内ＩＰネットワークにアクセスして、荷物を配送したことについて社内データベースを更新する。

【００２８】信頼ネットワーク要素（Ｔ）

Ｔは、信頼されるネットワーク要素を表す。Ｔは、Ｔが端末装置Ｕとの間のトラフィックに対するスヌーピング／挿入／変更の手段をＡに提供しないという限りで、Ｐにとって信頼できると判断する、インターネット内のルータである。本発明は、いったんトラフィックがインターネットコアに到達したら、そのトラフィックは、悪意のある攻撃に対して相当に安全であると仮定する。その理由は、この場合、ネットワークは少数の、定評のある、信頼された長距離会社のみによって運営されているからである。

【００２９】異なるＩＳＰは、Ｔが信頼される要素であるかどうかを判断するために、おそらくはそのユーザの要求およびＵの現在位置に依存して、異なるメカニズムおよびポリシーを適用することがある。Ｐが、インターネット内の信頼できるルータについての知識を有しない場合、Ｐ自体がＴの役割を受け持つ、すなわち、Ｐは自分のルータのうちの１つをＴとして選択すると仮定される。

【００３０】リモート通信相手（Ｒ）

Ｒは、リモート通信相手を表す。リモート通信相手は、端末Ｕが通信を要求する相手となる任意のリモートホストであることが可能である。例えば、リモート通信相手Ｒには、公衆インターネット上のサーバおよびその他のＩＰベースの装置、社内イントラネット上のサーバ、あるいは、社内イントラネットやプライベートＩＰネットワーク内のワークステーションやパーソナルコンピュータが含まれるが、これらには限定されない。

【００３１】仮定

本発明の目的のため、コンポーネントＵとＡの間は、ＡとＰの間とともに、互いに信頼関係がないと仮定される。具体的には、端末装置Ｕがリモート相手側Ｒと通信したいとき、Ｕは、Ｐからサービスを取得するために、単にその近傍内のアクセス局Ａを探索するだけである。通常、Ｕは、ＡとＵの間に信頼を生じうるような長期間継続する関係をＡとの間で有することはない。

【００３２】さらに、アクセス局Ａは、ＵやＰを信頼しないと仮定される。アクセス局Ａの主要な関心は、アクセス局Ａによって端末Ｕに提供されたリソースおよびサービスに対する償還を取得することに集中される。

【００３３】最後に、Ｐは、アクセス局Ａを信頼しない。Ｐは、その加入者Ｕが、Ａによって要求されたように実際にＡのリソースを使用していることを保証しなければならない。これは、アクセス局Ａが、存在しない端末ＵをＰに報告し、おそらくはＵからの虚偽のトラフィックさえ生成するような状況を回避するためである。そのような状況では、Ｐは、ＡがＰの真の加入者にサービスしていないのにＡに補償をすることになってしまう。ＡによってＵに対してなされるサービスについてのＰとＡの間の支払い手続きは、好ましくは、関連する当事者間の精算契約によって管理される。前述のように、ＵとＰの間の支払い手続きは、サービス契約によって管理され、定額制料金、あるいは、時間単位やトラフィック量単位で決定される使用料金に基づくことが可能である。

【００３４】本発明の応用

本明細書では、第三者所有のインフラストラクチャを通じてＩＰネットワーク（例えば、公衆インターネットや社内イントラネットのような）へのパブリックアクセスを提供するシステムおよび方法は、当業者には明らかなように、いくつかの具体的な方法で実現される。具体的には、本発明のシステムおよび方法は、全体として、ハ

ードウェア、ソフトウェアまたはその両方の組合せとして実現される。特に、本発明によって利用されるアクセスポイントあるいはその他のハードウェア要素は、プロセッサと、そのプロセッサの制御下にあるメモリとを有する。メモリには、プロセッサによって実行される命令（ソフトウェア）が提供され、これにより、プロセッサは、アクセス局、あるいはその他のハードウェアをさまざまな方法で動作させることが可能となる。同様に、アクセス局は、部分的に、ハードウェアおよびソフトウェアとして実現可能である。

【００３５】また、ＩＰネットワークへのアクセスを提供する本発明のシステムおよび方法は、ワイヤレスおよび有線のアクセスに関して同様に使用可能である。ここで、「ワイヤレス」とは、無免許周波数帯で動作する短距離技術を意味することも、より長距離の免許を受けた電波技術を意味することも可能である。

【００３６】さらに、ＩＰネットワークへのパブリックアクセスを提供する本発明のシステムは、ＩＰネットワークに接続するための有線、ワイヤレスまたはそれらの組合せの手段のいずれを用いて実現することも可能である。したがって、理解されるべき点であるが、「ＩＰネットワーク」あるいは「インターネット」という用語は、その最広義における「ＩＰに基づくネットワーク」を意味し、これには、公衆インターネット、社内イントラネット、プライベートまたはパブリックＬＡＮ、およびＩＰベースのアドホックネットワークが含まれるが、これらには限定されない。

【００３７】第三者のインフラストラクチャを用いて（インターネットのような）ＩＰネットワークへのアクセスを提供する本発明のシステムおよびメカニズムの利点は、ＩＳＰにとって利用可能であるとともに、自己の通信の必要のためにインターネットを使用する企業にも利用可能である。本発明の１つの利点は、ＩＳＰ／会社が、自己のアクセスネットワークを必要としないことである。したがって、ＩＳＰ／会社は、広い地域をアクセスポイントでカバーすることや、免許を要する周波数スペクトルのために高額な免許を取得する必要がない。

【００３８】本発明のシステムの例示的な応用分野には、以下の場合があるが、これらには限定されない。

・個人の家庭内のアクセス局が、ＷＬＡＮ（ＩＥＥＥ８０２．１１）、Ｂｌｕｅｔｏｏｔｈ（ＩＥＥＥ８０２．１５）、あるいはＨｉｐｅｒＬａｎなどの（これらには限定されない）ワイヤレス伝送標準を用いて、ワイヤレスアクセスを訪問者や近隣に提供する場合。

・ホテルや空港のような第三者によって所有され運営されるネットワークインフラストラクチャ内に実現された公共エリアアクセス局が、顧客のＩＳＰによって管理されるインターネットアクセスを顧客や訪問者に提供する場合。実現のためのワイヤレス標準には、ＷＬＡＮ（ＩＥＥＥ８０２．１１）、Ｂｌｕｅｔｏｏｔｈ（ＩＥＥＥ８０２．１５）およびＨｉｐｅｒＬａｎが含まれるが、これらには限定されない。

・アクセス局が、一時的に配備されリースされる場合。例えば、会議が、会議参加者に、その会議参加者のＩＳＰによって管理されるインターネットアクセスを与えるために、会議開催地でアクセス局をリースすることがある。実現のためのワイヤレス標準には、ＷＬＡＮ（ＩＥＥＥ８０２．１１）、Ｂｌｕｅｔｏｏｔｈ（ＩＥＥＥ８０２．１５）およびＨｉｐｅｒＬａｎが含まれるが、これらには限定されない。

【００３９】パブリックアクセスＬＡＮ環境に複数のワイヤレスアクセス技術を提供するため、さまざまなワイヤレス製品およびさまざまなタイプのワイヤレス事業者が共存可能であり、したがって、本発明の実施例は、さまざまなベンダからのワイヤレスＬＡＮカードとは独立の、相互運用可能なエアインタフェースであることに注意すべきである。

【００４０】［本発明の構成および動作］図１に本発明のコンポーネントを利用可能なネットワークを例示する。図１に示されるように、安全な（セキュア）トンネル（１）（破線で表す）が、端末ユーザＵ（３）と信頼されるノードＴ（５）の間で、アクセス局Ａ（７）を通じて確立される。いったん端末Ｕ（３）およびＩＳＰ　Ｐ（４）が認証されると、ＩＳＰ　Ｐは、信頼ノードＴ（５）を選択し、セッション鍵を端末Ｕ（３）および信頼ノード（５）に配送する（ＩＳＰ（４）、端末（３）および信頼ノードＴ（５）の間の破線で表す）。この秘密のセッション鍵は、アクセス局Ａには未知であるが、ＵとＴの間の暗号化を容易にするために使用されることになる。アクセス局Ａ（７）がデータをＵからＴへおよびＴからＵへ転送する能力とともに、ＵとＴの間の安全なトンネル（１）を確立することができる。この安全なトンネル（１）を用いて、端末Ｕ（３）は、暗号化されたデータパケットを信頼ノードＴ（５）に送信することが可能である。信頼ノードＴ（５）は、破線で表されるように、データパケットをＩＰネットワーク（９）へ、特に、リモートホスト（１０）へ転送する。

【００４１】図２は、安全なトンネル（１）の確立に必要な、端末Ｕ（３）、アクセス局Ａ（７）、ＩＳＰ　Ｐ（４）および信頼ノードＴ（５）の間の認証およびセッション鍵転送を示す同様のネットワークの図である。具体的には、端末Ｕ（３）およびＩＳＰ　Ｐ（４）は、両端に矢印のある長い破線で示されるように、アクセス局Ａ（７）を通じて認証チャレンジを互いに送信する。端末Ｕ（３）およびＩＳＰ　Ｐ（４）の両方の正しい認証の後、ＩＳＰ　Ｐ（４）は、セッション鍵を生成し、短い破線で示されるように、信頼ノードＴ（５）および端末Ｕ（３）に配送する。このセッション鍵を用いて、端末Ｕ（３）および信頼ノードＴ（５）は、データメッセージを暗号化し、アクセス局Ａ（７）を通る安全なトン

ネル（１）を通じてそれを転送する。しかし、データパケットの暗号化のため、アクセス局Ａ（７）は、そのデータパケットを復号したり変更したりすることはできない。換言すれば、信頼ノードＴ（５）がデータパケットをＩＰネットワーク（９）との間で転送し受信する間、アクセス局Ａ（７）は単に端末Ｕ（３）と信頼ノードＴ（５）の間の通路として作用するだけである。

【００４２】ＵとＰの相互認証

端末Ｕ（３）は、アクセス局Ａ（７）にアクセスすることができる（すなわち、端末Ｕ（３）とアクセス局Ａ（７）が、選択された通信媒体（有線またはワイヤレス）を通じてデータを交換することができる）地点に、スイッチオフモードで到着すると仮定する。さらに、端末Ｕ（３）およびＩＳＰ　Ｐ（４）は、公開鍵基盤[Pub Key]に参加していると仮定する。具体的には、公開鍵基盤への参加者は、「公開鍵」および「秘密鍵」という２つの鍵を有する。秘密鍵は、その参加者のみが知っており、他の当事者には決して明かされない。公開鍵は、誰もがどの参加者の公開鍵をも知っているように公開される。文献"Applied Cryptography: Protocols, Algorithms, and Source Code in C"で説明されている理由により、このような鍵は、一方の鍵（公開鍵または秘密鍵）で暗号化されたデータは他方の鍵（それぞれ、秘密鍵または公開鍵）では復号することができるが、他の鍵ではできないという性質を有する。

【００４３】次に、図２および図４を参照して、ユーザ端末Ｕ（３）が、たまたま端末Ｕ（３）の現在位置の近くにある信頼されないアクセス局Ａ（７）を用いて、自己のＩＳＰ　Ｐ（４）に対してどのようにしてサービスを要求するかについて説明する。

【００４４】ステップＳ１おいて、端末Ｕ（３）が起動され、そのネットワークインタフェースが初期化されると、端末Ｕ（３）はＩＰアドレスを取得するためにＤＨＣＰ（動的ホスト設定プロトコル）要求をネットワークにブロードキャストする。アクセス局Ａ（７）は、このブロードキャストの範囲内にある場合、このＤＨＣＰ要求を受信することになる。ＤＨＣＰは、コンピュータやワークステーションが、中央のサーバによって管理されるプールから一時的または永続的なＩＰアドレスを得ることを可能にするＩＰベースのプロトコルである。通常、ホストネットワークはＤＨＣＰサーバを動作させ、一方、ワークステーションやモバイル装置はＤＨＣＰクライアントを動作させる。ＤＨＣＰによれば、ＩＰアドレスを（モバイル装置のような）ノードにオンザフライで動的に割り当てることが可能となる。ＤＨＣＰに関する技術情報および背景的知識については、R. Dromsの"Dynamic Host Configuration Protocol (DHCP)"と題する文献を参照。注意すべき重要な点であるが、端末Ｕ（３）がアクセス局Ａ（７）と通信するために使用する技術に依存して、端末Ｕ（３）は、ＤＨＣＰ要求をブロードキャストする前に、アクセス局（７）とのある形式のアソシエーション（関連づけ）を作成することが必要な場合がある。このようなアソシエーションを確立する手続きは、ＩＥＥＥ８０２．１１技術に関する関連文書に規定されている。

【００４５】ステップＳ２において、アクセス局Ａ（７）が本発明のメカニズムをサポートする場合、アクセス局Ａ（７）は、「マジックＤＨＣＰ応答」(magic DHCP response)により端末Ｕ（３）に応答する。端末Ｕ（３）がどのようにして「マジック」と「非マジック」（標準）のＤＨＣＰ応答を区別するかについては後述する。「マジックＤＨＣＰ応答」の目的は、端末Ｕ（３）に対して、アクセス局Ａ（７）が本発明のメカニズムと互換性があることを示すことである。端末Ｕ（３）が標準すなわち非マジックＤＨＣＰ応答を受け取った場合、端末Ｕ（３）は、ＤＨＣＰの標準の動作モードに従ってＩＰアドレスを取得するだけであるため、本発明のメカニズムは利用可能ではないことを知る。いずれの場合でも、ＤＨＣＰ応答は、アクセス局Ａ（７）のＩＰアドレス（ゲートウェイとして識別される）と、端末Ｕ（３）のＩＰアドレス（クライアントＩＰアドレスとして識別される）を含む。

【００４６】ＤＨＣＰ応答は、さまざまな方法で、「マジックＤＨＣＰ応答」として定義されることが可能であり、それらはすべて、本発明の技術的範囲内に入る。例えば、ＤＨＣＰ応答は、値「１」に初期化された「ＡＰ」ＤＨＣＰオプションフィールドを含む場合に、「マジックＤＨＣＰ応答」とみなすことが可能である。ＤＨＣＰプロトコルは、新たなオプションフィールドの動的な導入を見込んでいる。「ＡＰ」ＤＨＣＰオプションフィールドの値が１であることは、端末Ｕ（３）が接続しようとしているアクセス局Ａ（７）が、本発明のメカニズムをサポートすることを示す。他方、「ＡＰ」ＤＨＣＰオプションフィールドがないか、１以外の値であることは、アクセス局Ａ（７）が本発明のメカニズムをサポートしないことを示す。

【００４７】別法として、「マジックＤＨＣＰ応答」は、予約されたＩＰアドレスを端末Ｕに割り当てるＤＨＣＰ応答として定義されることも可能である。例示のみの目的であるが、ＩＰアドレス１３８．１５．１０３．２２０（これは一般にＮＥＣＵＳＡの管理下にある）を、この目的のために使用可能である。このＩＰアドレスはＮＥＣ　ＵＳＡに割り当てられているため、他のネットワークによってＤＨＣＰクライアントに割り当てられることはできない。ＮＥＣ　ＵＳＡもまた、このアドレスを他の目的のために使用しないことを保証する。それゆえ、ＩＰアドレス１３８．１５．１０３．２２０が端末Ｕ（３）に割り当てられることは、アクセス局Ａ（７）が本発明のメカニズムをサポートすることを示す。他方、１３８．１５．１０３．２２０以外のＩＰア

ドレスが端末Ｕ（３）に割り当てられることは、アクセス局Ａ（７）が本発明のメカニズムをサポートしないことを示す。

【００４８】端末Ｕ（３）が単に動的に割り当てられたＩＰアドレスすなわち「非マジック」ＤＨＣＰ応答を受け取るだけである場合、端末Ｕ（３）には、ネットワークおよびアクセス局Ａ（７）が本発明をサポートしないことが確認される。したがって、端末Ｕ（３）は、第三者所有の信頼されないアクセス局Ａ（７）を通じて、端末Ｕ（３）のＩＳＰ　Ｐ（４）を利用したインターネットアクセスを取得することはできない。

【００４９】ステップＳ３ａにおいて、端末Ｕ（３）は、アクセス局Ａ（７）が存在すること、および、アクセス局Ａ（７）が本発明のメカニズムをサポートすることを知ると、識別パケットをアクセス局Ａ（７）に送る。このパケットは次のものを含む。

・端末Ｕ（３）が契約しているＩＳＰのＩＰアドレス。

・契約しているＩＳＰ　Ｐ（４）によって端末Ｕ（３）に以前に割り当てられた識別文字列あるいは番号。

・ＩＳＰ　Ｐ（４）を、端末Ｕ（３）が契約しているＩＳＰであるとして認証するために、端末Ｕ（３）によってランダムに生成されたチャレンジＣＨ__Ｕ。

【００５０】ステップＳ３ｂにおいて、アクセス局Ａ（７）は、ＩＳＰ認証パケットを端末Ｕ（３）から受け取ると、ローカル固有識別（ＬＵＩＤ：local unique identification）を端末Ｕ（３）に割り当てる。ＬＵＩＤは、アクセス局Ａ（７）が同時に複数の端末Ｕにサービスしているような状況で、メッセージやデータパケットを正しい端末Ｕ（３）と関連づける（照合する、組み合わせる）ために、アクセス局Ａ（７）によって利用される。ＬＵＩＤは、アクセス局Ａ（７）が正しい端末Ｕにデータを送信するのを助ける区別可能な識別属性であればよい。例として、ＬＵＩＤは、端末Ｕ（３）のＭＡＣアドレスとすることが可能であるが、これには限定されない。

【００５１】次に、アクセス局Ａ（７）は、修正されたＩＳＰ認証パケットをＩＳＰ　Ｐ（４）に転送する。アクセス局Ａ（７）は、端末ＵのＩＳＰ　Ｐ（４）のＩＰアドレスを知っている。これは、ステップＳ（３ａ）で端末Ｕ（３）からアクセス局Ａ（７）に送られたＩＳＰ識別パケットに、端末Ｕ（３）によって含められていたからである。修正されたＩＳＰ認証パケットは次のものを含む。

・アクセス局Ａ（７）のＩＰアドレス（ＩＳＰ　Ｐ（４）がデータをアクセス局Ａ（７）に転送することができるようにするため）。

・端末Ｕ（３）に割り当てられたＬＵＩＤ。

・端末Ｕ（３）の識別番号。

・端末Ｕ（３）がランダムに生成したチャレンジＣＨ__Ｕ。

【００５２】明確にしておかなければならない点であるが、端末Ｕ（３）の識別番号と端末Ｕ（３）のＬＵＩＤは２つの異なる無関係のＩＤである。識別番号は、ＩＳＰＰ（４）によって前もって端末Ｕ（３）に割り当てられたものである（例えば、これは、端末Ｕ（３）とＩＳＰ　Ｐ（４）が加入契約を結んだときに決定されたユーザ名である）。これに対して、ＬＵＩＤは、アクセス局Ａ（７）によって端末Ｕ（３）に動的に割り当てられ、アクセス局Ａ（７）が現在サービスを提供している端末Ｕ（３）を列挙するためにアクセス局Ａ（７）のみによって使用されるものである。端末Ｕ（３）およびＩＳＰ　Ｐ（４）のいずれも、アクセス局Ａ（７）がどのようにしてＬＵＩＤを選択し割り当てるかには影響を及ぼさない。

【００５３】ステップＳ４ａにおいて、ＩＳＰ　Ｐ（４）は、アクセス局Ａ（７）から修正されたＩＳＰ認証パケットを受け取ると、アクセス局Ａ（７）を通じてインターネットあるいはその他のサービスを取得することを端末Ｕ（３）が要求していることを知る。しかし、ＩＳＰ　Ｐ（４）は、ＩＳＰ認証パケットの発信者が正当な端末Ｕ（３）でありＩＳＰ　Ｐ（４）と契約しているかどうかを確かめることができない。例えば、ＩＳＰ認証パケットは、ＩＳＰ　Ｐ（４）と加入契約をしていないユーザから送られたものかもしれない。あるいは、アクセス局（７）が、サービスを提供することを必要とせずにＩＳＰから補償を得る目的でユーザになりすまして要求を生成することによって、悪意をもってふるまっているかもしれない。そこで、ＩＳＰ　Ｐ（４）は、端末Ｕ（３）がＩＳＰ　Ｐ（４）の真正な加入者であることを確かめるために、端末Ｕ（３）の識別（身元）を認証しなければならない。

【００５４】端末Ｕ（３）を認証するため、ＩＳＰ　Ｐ（４）は、端末Ｕ（３）によって正しく応答されるときに端末Ｕ（３）の識別を確認することになるチャレンジＣＨ__Ｐを生成する。注意すべき点であるが、このようなチャレンジは通常、乱数ジェネレータによって生成される大きい数または文字列である。

【００５５】この際、ＩＳＰ　Ｐ（４）は、ステップ（３ａ）で端末Ｕ（３）によって生成されたチャレンジＣＨ__Ｕに対する応答も行う。ＣＨ__Ｕは、単に、ＩＳＰ　Ｐ（４）の秘密鍵で暗号化されて端末Ｕ（３）に送られるだけであるので、端末Ｕ（３）は、ＩＳＰ　Ｐ（４）の公開鍵を用いてこのメッセージを復号することができる。もとのＣＨ__Ｕメッセージが判明した場合、端末Ｕ（３）には、ＩＳＰＰ（４）の真正が確かめられる（すなわち、ＩＳＰ　Ｐ（４）は端末Ｕ（３）に認証される）。

【００５６】さらに、ＩＳＰ　Ｐ（４）は、端末Ｕ（３）のセキュリティ要求およびアクセス局Ａ（７）の位置に依存して、信頼ネットワークノードＴ（５）を選

択する。最後に、ＩＳＰ　Ｐ（４）は、次の内容を有するパケットをアクセス局Ａ（７）に送る。
・端末Ｕ（３）のチャレンジに対するＩＳＰ　Ｐ（４）の応答。これは、ＣＨ＿ＵをＩＳＰ　Ｐ（４）の秘密鍵で暗号化したものである。
・端末Ｕ（３）を認証するための、ＩＳＰ　Ｐ（４）がランダムに生成したチャレンジＣＨ＿Ｐ。
・信頼ノードＴ（５）のＩＰアドレス。
・アクセス局Ａ（７）によって端末Ｕ（３）に割り当てられたＬＵＩＤ。
【００５７】ステップＳ４ｂで、アクセス局Ａ（７）は、ＩＳＰ　Ｐ（４）からユーザ認証パケットを受け取ると、修正されたユーザ認証パケットを端末Ｕ（３）に転送する。この修正されたユーザ認証パケットは次のものを含む。
・端末Ｕ（３）のチャレンジに対するＩＳＰ　Ｐ（４）の応答。これは、ＣＨ＿ＵをＩＳＰ　Ｐ（４）の秘密鍵で暗号化したものである。
・端末Ｕ（３）を認証するための、ＩＳＰ　Ｐ（４）がランダムに生成したチャレンジＣＨ＿Ｐ。
・アクセス局Ａ（７）が同時に複数のユーザＵ（３）にサービスしている場合、端末Ｕ（３）に割り当てられたＬＵＩＤもユーザ認証パケットに含められる。前述のように、ＬＵＩＤは、どの端末Ｕ（３）がデータパケットを受け取るべきかをアクセス局Ａ（７）が判断するのを助ける。
【００５８】ステップＳ５ａで、端末Ｕ（３）は、ＩＳＰ　Ｐ（４）によってＰの公開鍵で暗号化された、チャレンジＣＨ＿Ｕに対するＩＳＰ　Ｐ（４）の応答を、ＩＳＰＰ（４）の公開鍵を用いて復号し確認する。端末Ｕ（３）が、ＩＳＰ　Ｐ（４）の公開鍵を用いて、チャレンジＣＨ＿Ｕに対するＩＳＰ　Ｐ（４）の応答を復号することに成功した場合、端末Ｕ（３）には、暗号化された応答が実際にＩＳＰ　Ｐ（４）によって生成されたものであることが確かめられ、これによりＩＳＰ　Ｐ（４）の識別が認証される。
【００５９】この時点で、端末Ｕ（３）は、端末Ｕ（３）の識別を確認し認証するための、ＩＳＰ　Ｐ（４）によって生成されたチャレンジＣＨ＿Ｐに対する応答の生成も行う。ＩＳＰ　Ｐ（４）のチャレンジＣＨ＿Ｐに応答して、端末Ｕ（３）は、ＩＳＰ　Ｐ（４）のチャレンジＣＨ＿Ｐを、端末Ｕ（３）の秘密鍵で暗号化する。その後、端末Ｕ（３）は、次の内容を有するメッセージをアクセス局Ａ（７）に送る。
・ＩＳＰ　Ｐのチャレンジ＿Ｐに対する端末Ｕ（３）の応答。
【００６０】ステップＳ５ｂにより、アクセス局Ａ（７）は、ステップＳ５ａで生成された端末Ｕ（３）からのメッセージを受け取り、それをＩＳＰ　Ｐ（４）に転送する。必ずしも必要ではないが、アクセス局Ａ（７）が端末Ｕ（３）のＬＵＩＤをＩＳＰ　Ｐ（４）へのメッセージに含めると有益なことがある。その場合、将来、（ＩＳＰ　Ｐ（４）からアクセス局Ａ（７）を通じて端末Ｕ（３）に送らなければならないデータについて）ＩＳＰ　Ｐ（４）が正しい端末Ｕ（３）をアクセス局Ａ（７）に指示することが容易になる。
【００６１】ステップＳ６ａおよびＳ６ｂで、ＩＳＰ　Ｐ（４）は、チャレンジＣＨ＿Ｐに対する端末Ｕ（３）の応答が、正当な端末Ｕ（３）によって生成されたことを確認する。端末Ｕ（３）を認証するために、ＩＳＰ　Ｐ（４）は、チャレンジＣＨ＿Ｐに対する応答を端末Ｕ（３）の公開鍵で復号する。復号された応答が、ＩＳＰ　Ｐ（４）のもとのチャレンジＣＨ＿Ｐとなった場合、ＩＳＰ　Ｐ（４）には、端末Ｕ（３）が正当な加入者であり、ＩＳＰ　Ｐ（４）と契約していることが確かめられる。
【００６２】ここで、ＩＳＰ　Ｐ（４）は、端末Ｕ（３）と信頼ノードＴ（５）が後で端末Ｕ（３）と信頼ノードＴ（５）の間のトラフィックを暗号化して、端末Ｕ（３）と信頼ノードＴ（５）の間に安全なトンネル（１）を確立するために使用することになるセッション鍵を生成する。セッション鍵とともに、安全なトンネルの有効期間を決定するタイムアウト値が、端末Ｕ（３）および信頼ノードＴ（５）の両方に伝えられる。
【００６３】ステップＳ６ａで生成され、ＩＳＰ　Ｐ（４）から信頼ノードＴ（５）に送られるメッセージは、次の情報を含む。
・セッション鍵^{PT}。これは、セッション鍵を、信頼ノードＴ（５）の公開鍵およびＩＳＰ　Ｐ（４）の秘密鍵で暗号化したものである。注意すべき重要な点であるが、セッション鍵は信頼ノードＴ（５）の公開鍵で暗号化されるため、信頼ノードＴ（５）のみが（その秘密鍵を用いて）それを復号することができる。セッション鍵はＩＳＰ　Ｐ（４）の秘密鍵で暗号化されるため、信頼ノードＴ（５）は、それが実際にＩＳＰ　Ｐ（４）から来たことを（ＩＳＰ　Ｐ（４）の周知の公開鍵を用いて）確認することができる。
・安全なトンネル（１）の有効期間を決定するタイムアウト値（詳細は後述）。
・アクセス局Ａ（７）のＩＰアドレス。
・アクセス局Ａ（７）によって端末Ｕ（３）に割り当てられた、端末Ｕ（３）のＬＵＩＤ。
【００６４】ステップＳ６ｂで生成されたメッセージは、アクセス局Ａ（７）を通じてＩＳＰ　Ｐ（４）から端末Ｕ（３）に送られる。すなわち、これは、まずＩＳＰ　Ｐ（４）からアクセス局Ａ（７）に送られた後、アクセス局Ａ（７）によって端末Ｕ（３）に転送される。このメッセージは、次の情報を含む。
・セッション鍵^{UT}。これは、セッション鍵を、端末Ｕ（３）の公開鍵およびＩＳＰ　Ｐ（４）の秘密鍵で暗号

化したものである。注意すべき重要な点であるが、セッション鍵は端末Ｕ（３）の公開鍵で暗号化されるため、端末Ｕ（３）のみが（その秘密鍵を用いて）それを復号することができる。セッション鍵はＩＳＰＰ（４）の秘密鍵で暗号化されるため、端末Ｕ（３）は、それが実際にＩＳＰＰ（４）から来たことを（ＩＳＰ　Ｐ（４）の周知の公開鍵を用いて）確認することができる。

・安全なトンネル（１）の有効期間を決定するタイムアウト値。

・アクセス局Ａ（７）によって端末Ｕ（３）に割り当てられた、端末Ｕ（３）のＬＵＩＤ。注意すべき重要な点であるが、ＬＵＩＤは、アクセス局Ａ（７）が、メッセージを正しい端末Ｕ（３）に転送するためにのみ必要とされる。この情報フィールドは、アクセス局Ａ（７）から端末Ｕ（３）に送られる最終的なメッセージでは随意に省略することができる。

【００６５】アクセス局Ａ（７）を通じての端末Ｕ（３）と信頼ノードＴ（５）の間の安全なトンネル（１）の生成

いったん端末Ｕ（３）およびＩＳＰ　Ｐ（４）が認証されると、端末Ｕ（３）がＩＰパケットをアクセス局Ａ（７）に送ることができ、さらにそれをアクセス局Ａ（７）が信頼ノードＴ（５）に転送することができる。また、その逆も可能である（信頼ノードＴ（５）がＩＰパケットをアクセス局Ａ（７）に送ることができ、その後それをアクセス局Ａ（７）が端末Ｕ（３）に転送することができる）。その結果、端末Ｕ（３）と信頼ノードＴ（５）の間に（アクセス局Ａ（７）を通じて）安全なトンネル（１）が確立される。この安全なトンネル（１）の目的は、端末Ｕ（３）と信頼ノードＴ（５）の間の物理リンクをエミュレートすることである。さらに、端末Ｕ（３）および信頼ノードＴ（５）は両方とも（ＩＳＰ　Ｐ（４）によって生成された）同じセッション鍵を有するため、安全なトンネル（１）を通るトラフィックはこのセッション鍵で暗号化することが可能である。安全なトンネルを通るパケットを暗号化することにより、端末Ｕ（３）と信頼ノードＴ（５）の間に位置するネットワーク要素（例えば、アクセス局Ａ（７））は、端末Ｕ（３）や信頼ノードＴ（５）によって検出されずにＩＰパケットの追加、変更あるいは除去を行うことは不可能となる。

【００６６】アクセス局Ａ（７）は、メッセージを信頼ノードＴ（５）に送るときにはいつも、そのメッセージを発信した端末Ｕ（３）のＬＵＩＤを含める。ＬＵＩＤは、アクセス局Ａ（７）のＩＰアドレスとともに、信頼ノードＴ（５）が端末Ｕ（３）を識別するために使用可能なグローバルに一意的なＩＤを生成する。

【００６７】さらに、信頼ノードＴ（５）は、（端末Ｕ（３）への最終的配送のために）アクセス局Ａ（７）に送るのと同じＬＵＩＤをメッセージに含める。アクセス局Ａ（７）は、このＬＵＩＤを用いて、メッセージの転送先とすべき正しい端末Ｕ（３）を決定することができる。ＬＵＩＤは、端末Ｕ（３）にとっては重要でないため、アクセス局Ａ（７）は、信頼ノードＴ（５）から端末Ｕ（３）に転送するメッセージからそれを随意に除去することも可能である。

【００６８】端末ＵとＩＰネットワークの間のデータ転送

次に、図２および図５を参照して、端末Ｕ（３）とＩＰネットワーク（９）（例えば、インターネットや社内イントラネット）の間のデータ転送について説明する。注意すべき重要な点であるが、図４が、端末Ｕ（３）、アクセス局Ａ（７）、ＩＳＰ　Ｐ（４）、および信頼ノードＴ（５）の間のメッセージシーケンスを示したのとは異なり、図５は、端末Ｕ（３）、アクセス局Ａ（７）、信頼ノードＴ（５）およびインターネット（９）の間のメッセージシーケンスを示す。

【００６９】図５から理解されるとともに、すでに説明したように、端末Ｕ（３）と信頼ネットワークノードＴ（５）の間でアクセス局Ａ（７）を通じてデータを送信するために、安全なトンネル（１）が確立される。端末Ｕ（３）、アクセス局Ａ（７）、および信頼ノードＴ（５）が安全なトンネル（１）を通じてＩＰパケットを交換することができることにより、これ以上ＩＳＰ　Ｐ（４）が関与することは不要となる（ＩＳＰ　Ｐ（４）の関与は、生成されたセッション鍵が端末Ｕ（３）および信頼ノードＴ（５）に安全に配送されたときに終了する）。

【００７０】一般に、安全なトンネル（１）を通じてＩＰパケットを送信する前に、端末Ｕ（３）は、信頼ノードＴ（５）からＩＰアドレスを取得するために、安全なトンネル（１）を通じて第２のＤＨＣＰ要求を信頼ノードＴ（５）に転送する。注意すべき重要な点であるが、安全なトンネル（１）は、端末Ｕ（３）と信頼ノードＴ（５）の間の物理リンクをエミュレートする。安全なトンネル（１）が確立された後、端末Ｕ（３）は次の２つのネットワークインタフェースを有する（それぞれＩＰアドレスを必要とする）。

【００７１】１）　端末Ｕ（３）をアクセス局Ａ（７）と接続する物理インタフェース（例えば、イーサーネットカードや８０２．１１ワイヤレスＬＡＮカード）。端末Ｕ（３）は、第１のＤＨＣＰ要求を送出することによって、このインタフェースに対するＩＰアドレスを取得した。このＤＨＣＰ要求は、アクセス局Ａ（７）によって受信され応答された。

【００７２】２）　端末Ｕ（３）を信頼ノードＴ（５）と接続する、安全なトンネル（１）への論理インタフェース。端末Ｕ（３）は、安全なトンネル（１）を通じて第２のＤＨＣＰ要求をブロードキャストすることによって、このインタフェースに対する別のＩＰアドレスを取

得しなければならない。ただし、この第２のＤＨＣＰ要求は、信頼ノードＴ（５）によって受信され応答される。

【００７３】第２のＩＰアドレスを信頼ノードＴ（５）から取得することにより、端末Ｕ（３）は、グローバルインターネット（９）によって信頼ノードＴ（５）へとルーティングされる送信元アドレスを有するＩＰパケットを生成することが可能となる。さらに、信頼ノードＴ（５）は、その宛先アドレスを有するＩＰパケットを、信頼ノードＴ（５）と端末Ｕ（３）の間のトンネルを通じて端末Ｕ（３）に転送することが可能となる。

【００７４】第２のＤＨＣＰ要求に関するメカニズムについて以下で説明する。端末Ｕ（３）は、（自分（端末Ｕ（３））と信頼ノードＴ（５）との間に確立した）安全なトンネル（１）を、追加の（論理）ネットワークインタフェースとして利用可能にするために、第２のＤＨＣＰ要求を生成する。ステップ７ａに示すように、端末Ｕ（３）は、このＤＨＣＰ要求を、端末Ｕ（３）と信頼ノードＴ（５）の間で共有されるセッション鍵で暗号化する。次に、端末Ｕ（３）は、暗号化されたＤＨＣＰ要求を、新たなＩＰパケット「Ｙ」のペイロードフィールドに入れる（すなわち、Ｙ［ＤＨＣＰ要求／セッション鍵］）。「Ｙ」ＩＰパケットは、信頼ノードＴ（５）のＩＰアドレスをその宛先アドレスとし、アクセス局Ａ（７）のアドレスをその送信元アドレスとする。「Ｙ」ＩＰパケット（Ｙ［ＤＨＣＰ要求／セッション鍵］）は、アクセス局Ａ（７）に転送される。アクセス局Ａ（７）は、「Ｙ」ＩＰパケットを信頼ノードＴ（５）に転送するが、パケット内の内容を復号することはできない。アクセス局Ａ（７）は正しいセッション鍵を有しないからである。注意すべき重要な点であるが、アクセス局Ａ（７）は、「Ｙ」ＩＰパケットを信頼ノードＴ（５）に転送するときに、前述したように、端末Ｕ（３）のＬＵＩＤを「Ｙ」ＩＰパケットに付加することが可能である。

【００７５】ステップＳ７ｂにおいて、信頼ノードＴ（５）は、アクセス局Ａ（７）を通じて、暗号化されたＤＨＣＰ要求を含む「Ｙ」ＩＰパケットを端末Ｕ（３）から受け取ると、ＤＨＣＰ要求を復元し、ＩＰアドレスを端末Ｕ（３）に割り当て、端末Ｕ（３）に対するＤＨＣＰ応答を生成する。明らかなように、このＤＨＣＰ要求によって端末Ｕ（３）に割り当てられるＩＰアドレスは、グローバルインターネット（９）がメッセージを信頼ノードＴ（５）にルーティングするために使用するＩＰアドレスである。その後、このＤＨＣＰ応答は、セッション鍵で暗号化されてアクセス局Ａ（７）に転送され、アクセス局Ａ（７）はこの応答を端末Ｕ（３）に送る。この間、アクセス局Ａ（７）は応答の内容を復号することはできない。

【００７６】端末Ｕ（３）は、暗号化されたＤＨＣＰ応答を受け取ると、ＩＰアドレスを取得する。このＩＰアドレスは、グローバルインターネット（９）が信頼ノードＴ（５）にルーティングし、信頼ノードＴ（５）が端末Ｕ（３）に（アクセス局Ａ（７）を通じての、安全なトンネル（１）を通って）転送するものである。明確にするため、注意すべき点であるが、上記のＤＨＣＰ応答に含まれるＩＰアドレスは、信頼ノードＴ（５）自体のＩＰアドレスではなく、グローバルインターネット（９）が信頼ノードＴ（５）にルーティングするＩＰアドレスである。信頼ノードＴ（５）は、このＩＰアドレスを宛先アドレスとして有するメッセージを受け取ると、信頼ノードＴ（５）がメッセージの最終受信者ではなく、端末Ｕ（３）である最終宛先へメッセージを転送することになっていることを容易に判断することができる（すなわち、信頼ノードＴ（５）はルータとして作用する）。信頼ノードＴ（５）は、端末Ｕ（３）のＤＨＣＰ要求に対して、前記ＩＰアドレスを含むＤＨＣＰ応答により応答するとき、前記ＩＰアドレスを端末Ｕ（３）の識別および対応するアクセス局Ａ（７）と関連づけるレコードを保持する。この情報により、信頼ノードＴ（５）は、グローバルインターネット（９）から受け取るあらゆるＩＰパケットについて、次の情報を判定することが可能となる。

・パケットの転送先となるべき関連づけられた端末Ｕ（３）。

・信頼ノードＴ（５）をその特定の端末Ｕ（３）と接続する安全なトンネル（１）。

・安全なトンネル（１）を通じての送信用にパケットを暗号化するために使用しなければならないセッション鍵。

・安全なトンネル（１）が通り、暗号化されたパケットの転送先となるべき、関連づけられたアクセス局Ａ（７）。

【００７７】ステップＳ８ａにおいて、端末Ｕ（３）と信頼ノードＴ（５）との間の（安全なトンネル（１）を通じての）パケットトラフィックの送信について詳細に説明する。この説明は、データパケットの詳細な内訳を示す図３を参照することにより補足される。具体的には、端末Ｕ（３）は、新たなＩＰパケットＸ（１１）を作成する。図３からわかるように、データパケットＸ（１１）のパケットヘッダ（１２）は、リモートホストＲ（１０）（図１に示されるような）の宛先アドレスと、端末Ｕ（３）からという送信元アドレスを有する。特に、送信元アドレスは、端末Ｕ（３）の要求に対して信頼ノードＴ（５）から端末Ｕ（３）に返されるＤＨＣＰ　ＩＰアドレスである。

【００７８】次に、ＩＰパケット（１１）全体（データパケットＸおよびヘッダを含む）が、端末Ｕ（３）と信頼ノードＴ（５）の間で共有されるセッション鍵で暗号化され、データパケットＹ（１６）のペイロード（１

４）として格納される（Ｙ［Ｘ／ｋｅｙ］）。ここで、暗号化されたＩＰパケットＹ［Ｘ／ｋｅｙ］（１６）のヘッダ（１８）宛先アドレスは、信頼ノードＴ（５）のＩＰアドレスであり、このＩＰパケットの送信元アドレスは、端末Ｕ（３）に割り当てられるマジックＤＨＣＰアドレスである。

【００７９】ステップＳ８ａに示されるように、アクセス局Ａ（７）は、暗号化されたＩＰパケットＹ［Ｘ／ｋｅｙ］（１６）を受信する。アクセス局Ａ（７）は、もちろん、暗号化されたＩＰパケットＹ［Ｘ／ｋｅｙ］（１６）内に含まれる内容（すなわちＸ）を復元したり操作したりすることはできない。そこで、アクセス局Ａ（７）は、暗号化されたＩＰパケットＹ［Ｘ／ｋｅｙ］（１６）内の送信元アドレスフィールドをアクセス局Ａ（７）のＩＰアドレスで置き換えて、修正されたパケットＹ′［Ｘ／ｋｅｙ］を作成することにより、暗号化されたＩＰパケットＹ［Ｘ／ｋｅｙ］（１６）を信頼ノードＴ（５）に転送する。さらに、アクセス局Ａ（７）は、どの端末Ｕ（３）がもとのパケットＸ（１１）を送信したかを信頼ノードＴ（５）が判断するのを助けるために、端末Ｕ（３）のＬＵＩＤを修正されたＩＰパケットＹ′［Ｘ／ｋｅｙ］に付加することが可能である。信頼ノードＴ（５）は、メッセージを復号する正しいセッション鍵を選択するためには、どの端末Ｕ（３）がパケット（１１）を送信したかを知らなければならない。

【００８０】ステップＳ８ｂにより、信頼ノードＴ（５）は、もとのデータパケットＸ（１１）を復元する。データパケットＸ（１１）はインターネット（９）に転送される。同様に、端末Ｕ（３）宛のインターネット（９）からのデータパケットは、ステップＳ８ｂに示されるように、信頼ノードＴ（５）によって受信される。信頼ノードＴ（５）は、セッション鍵を用いてデータパケットを暗号化した後、ステップＳ８ａに示されるように、暗号化されたパケットをアクセス局Ａ（７）に転送する。アクセス局Ａ（７）は、ＬＵＩＤに基づいて、メッセージを正しい端末Ｕ（３）に転送する。

【００８１】別法として、ＩＰ送信元アドレスと送信元ポート番号の一意的な２つ組をトンネルにマッピングするＮＡＴ（ネットワークアドレス変換）メカニズムが使用される場合には、ステップＳ７を省略することも可能である。その場合、端末Ｕ（３）によって送信され信頼ノードＴ（５）によって受信される最初のデータパケットＸ（１１）が、端末Ｕ（３）を信頼ノードＴ（５）と関連づけることになる。そして、トンネルと外部インターネット接続との間で接続パラメータをマッピングするデータ構造が作成される。

【００８２】トンネル解放とタイムアウト

タイムアウトメカニズムは、端末Ｕ（３）と信頼ノードＴ（５）の間に確立された安全なトンネル（１）に関連するリソースの解放をトリガする。前記リソースは、端末Ｕ（３）、アクセス局Ａ（７）および信頼ノードＴ（５）に存在する。タイムアウトおよびトンネル解放を制御するタイミングメカニズムは、トンネルの両端（すなわち、端末Ｕ（３）内および信頼ノードＴ（５）内）に配置されることが可能である。タイミングメカニズムは、端末Ｕ（３）および信頼ノードＴ（５）へのセッション鍵の配送の成功時にセットされる。それぞれのタイミングメカニズムのタイマ値は、ＩＳＰ　Ｐ（４）と端末Ｕ（３）の間、およびＩＳＰ　Ｐ（４）と信頼ノードＴ（５）の間で転送されるセッション鍵とともに渡されることが可能である。

【００８３】端末Ｕ（３）へのサービス提供と、提供される関連リソースとを制御する別個のタイマが、アクセス局Ａ（７）で維持される。このタイマは、トンネル（１）が確立されると、すなわち、セッション鍵が転送されるとすぐに開始される。好ましくは、端末Ｕ（３）宛のタイムアウト値が、このタイマのプリセット値として使用される。タイムアウト時に、サービス提供は停止され、アクセス局Ａ（７）におけるしソースは解放される。正しい動作を保証するため、データ転送の場合であっても、アクセス局Ａ（７）にあるタイマのタイムアウト値は、トンネル（１）のタイムアウトのタイムアウト値より大きくすべきである。

【００８４】トンネル（１）の有効期間を延長するためには、端末Ｕ（３）は、タイマが満期になる前に、新たなサービスおよびＩＳＰ　Ｐ（４）との再認証要求を呼び出すことが可能である。再認証要求は、アクセス局Ａ（７）によって端末Ｕ（３）に提供される接続サービスについて、端末Ｕ（３）の真正と、計測された継続時間情報を保証する。端末Ｕ（３）および信頼ノードＴ（５）にあるタイマが満期になると、トンネルリソースは、それぞれのネットワーク要素から解放される。

【００８５】しかし、遅いデータ転送中のトンネルの正しい動作および維持を保証するために、各タイマは、安全時間マージン(safety time margin)を有することも可能である。安全時間マージンは、タイマに追加時間のバッファを割り当てることにより、リソースが解放されたり再認証要求がなされたりする前に、遅いデータ転送が完了するようにする。

【００８６】課金

アクセス局Ａ（７）が端末Ｕ（３）にサービスを提供した時間の長さに基づくアカウンティング方法も実現される。ある計測単位を利用して、アクセス局Ａ（７）が端末Ｕ（３）にサービスを提供した期間を計上する。計測単位は、端末Ｕ（３）、信頼ノードＴ（５）およびアクセス局Ａ（７）に渡されるタイムアウト値によって決定される。計測単位は、数十秒から数分までの範囲にある時間単位とすることが可能である。通常、計測単位は、ＩＳＰ　Ｐ（４）とアクセス局Ａ（７）の間のサービス契約、および、ＩＳＰ　Ｐ（４）と端末Ｕ（３）の間の

契約によって規定される。タイムアウト値は、再認証手続きの呼出しによって引き起こされる時間粒度とシグナリングおよび処理のオーバーヘッドとによって影響を受けることがある。タイミングメカニズムは、システムの正しい動作にとって必要であるため、課金情報は、定期的な再認証手続き中に伝達されるタイムアウト値から導出することが可能である。

【００８７】ＩＳＰ　Ｐ（４）が、端末Ｕ（３）によって利用されたリソースについてアクセス局Ａ（７）に補償するとともにタイマ値に基づいて端末Ｕ（３）に課金するように、タイマ値はＩＳＰ　Ｐ（４）によって生成され配送されることも可能であるが、端末Ｕ（３）が、プリペイドオプションによりＩＳＰサービスを取得することも可能である。例えば、端末Ｕ（３）は、与えられた期間ｔの間だけ、アクセス局Ａ（７）により提供されるリソースに端末Ｕ（３）がアクセスしそれを利用することを許可するプリペイド加入契約をＩＳＰ　Ｐ（４）と結ぶことが可能である。期間ｔは、ＩＳＰ　Ｐ（４）から端末Ｕ（３）が購入する計測単位（例えば分単位）の量に対応する。通常、それぞれの認証および再認証の成功により、タイムアウト間隔（例えば１分）と等価な金額分がデクリメントされる。プリペイド時間単位が使い果たされると、ＩＳＰ　Ｐ（４）は、端末Ｕ（３）に対して、再認証や新たなタイムアウト値の配送を行わない。その後、アクセス局Ａ（７）、信頼ノードＴ（５）および端末Ｕ（３）にあるタイマが満期になり、トンネル（１）は関連するリソースとともに解放される。

【００８８】

【発明の効果】以上説明したように、本発明によれば、端末と第三者所有の信頼されない（非信頼）アクセス局との間に接続を確立し、続いて、端末と契約しているインターネットサービスプロバイダ（ＩＳＰ）へＩＳＰ認証要求を送信する。ＩＳＰと端末が正しく認証された後、端末と信頼ゲートウェイとの間に信頼された接続を確立する。こうして確立された接続を安全なトンネルとして利用することにより、ＩＳＰは、非信頼アクセス局を通じて端末に対して安全なインターネットアクセスを提供することができる。

【００８９】こうして公衆インターネットやプライベートＬＡＮのようなパブリックまたはプライベートＩＰネットワークへのアクセスのために、既存のインフラストラクチャの共有を可能にするメカニズムを提供することができる。特に、インフラストラクチャの所有者はそのリソースを異なるＩＳＰへ短期間ベースでリースし、１つのＩＳＰはこれらリソースを用いて加入者にインターネットサービスを提供する。ＩＳＰは、課金、帯域管理およびｅメールなど、加入者に提供されるインターネットサービスの全ての側面を制御する。また、ＩＳＰは暗号化によって、加入者のプライバシーを保証する。既存のネットワーク・インフラストラクチャからのネットワークリソースのリースによって、ＩＳＰにとっては高価なアクセスインフラ自体を構築する必要がなくなり、他方、インフラストラクチャの所有者にとってはインフラから付加的な報酬を発生させる機会が与えられる。重要なのは、ユーザにとってもＩＳＰによっても、ＩＰネットワークへのアクセスを実行するためのアクセス局を信頼する必要がない（すなわちアクセス局は非信頼である）ことである。

【図面の簡単な説明】

【図１】本発明によるネットワークのモデルを示す図である。

【図２】本発明の実施例のコンポーネント間の情報フローを示す図である。

【図３】アクセス局Ａを通じてユーザ（Ｕ）から信頼ネットワーク要素Ｔに転送されるトンネル化データパケットを示す図である。

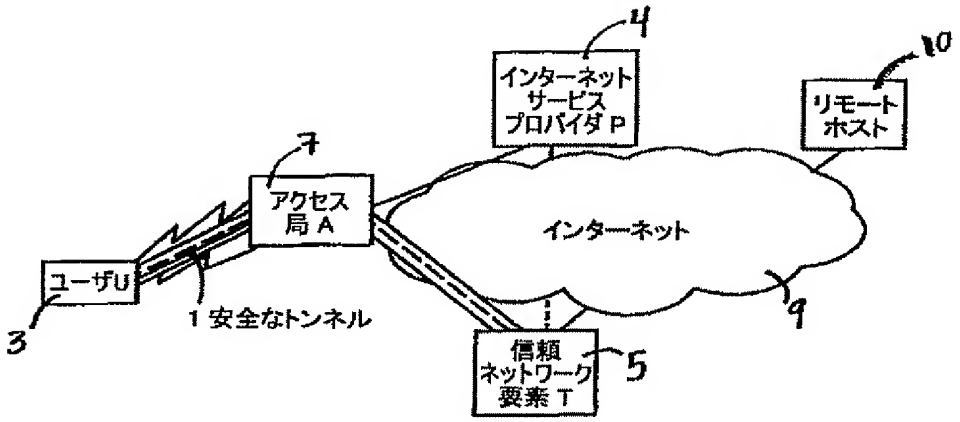
【図４】セッション鍵の認証および配送のメッセージシーケンスを示す図である。

【図５】アソシエーションおよびデータ転送のメッセージシーケンスを示す図である。

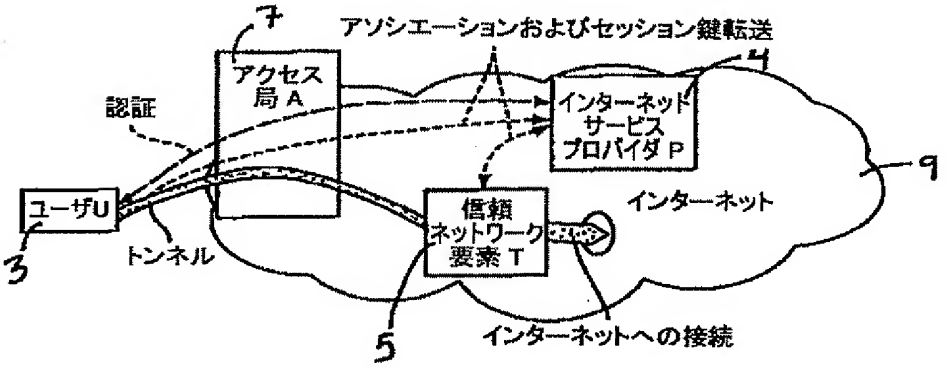
【符号の説明】

１　安全なトンネル
３　端末ユーザＵ
４　ＩＳＰ　Ｐ
５　信頼ノードＴ
７　アクセス局Ａ
９　ＩＰネットワーク
１０　リモートホスト
１１　データパケットＸ
１６　データパケットＹ

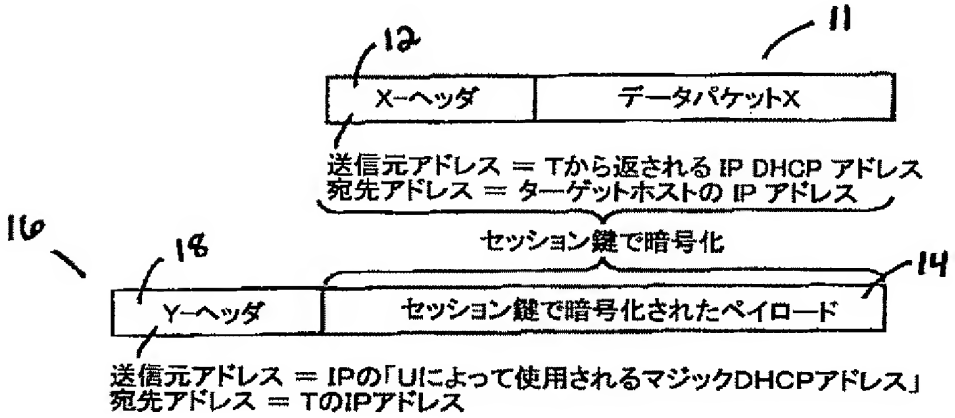
【図１】


4
インターネット
サービス
プロバイダ P
10
リモート
ホスト
7
アクセス
局 A
インターネット
ユーザU
3
1 安全なトンネル
9
信頼
ネットワーク
要素 T
5

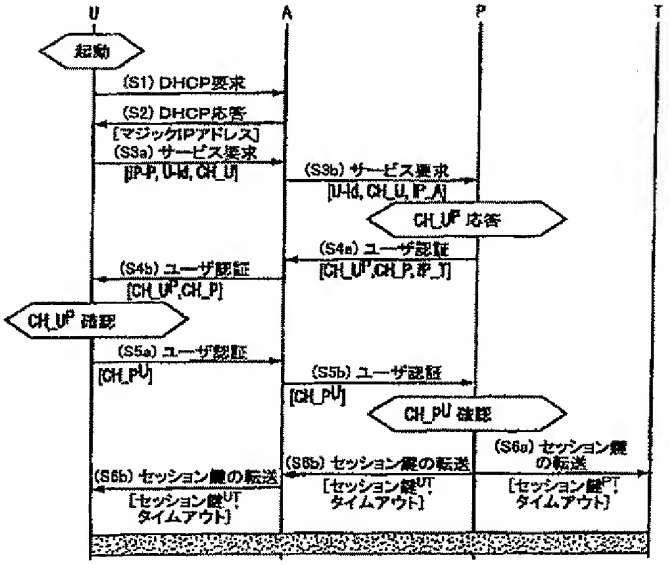
【図２】


7
アソシエーションおよびセッション鍵転送
アクセス
局 A
4
認証
インターネット
サービス
プロバイダ P
9
ユーザU
3
トンネル
信頼
ネットワーク
要素 T
インターネット
5
インターネットへの接続

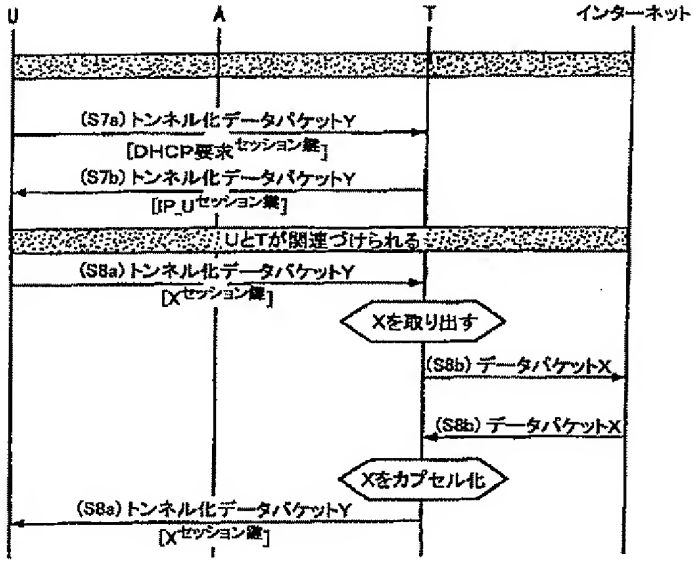
【図３】


12
11
X-ヘッダ
データパケットX
送信元アドレス ＝ Tから返される IP DHCP アドレス
宛先アドレス ＝ ターゲットホストの IP アドレス
セッション鍵で暗号化
16
18
14
Y-ヘッダ
セッション鍵で暗号化されたペイロード
送信元アドレス ＝ IPの「Uによって使用されるマジックDHCPアドレス」
宛先アドレス ＝ TのIPアドレス

【図４】



【図５】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I		テーマコード（参考）
Ｈ０４Ｌ 12/56		Ｈ０４Ｌ 9/00	６０１Ｂ	
Ｈ０４Ｑ 7/38		Ｈ０４Ｂ 7/26	１０９Ｒ	

(72)発明者　トーマス　クーネル
アメリカ合衆国，ニュージャージー　08540　プリンストン，４　インディペンデンス　ウエイ，エヌ・イー・シー・ユー・エス・エー　インク内

(72)発明者　ワォルフ　ミューラー
アメリカ合衆国，ニュージャージー　08540　プリンストン，４　インディペンデンス　ウエイ，エヌ・イー・シー・ユー・エス・エー　インク内

Ｆターム(参考)　5B085 AC04 AE01 AE29 BA06 BG02 BG07
5B089 GB01 HB18 KA17 KB13
5J104 AA07 KA02 NA03 PA07
5K030 GA15 HA08 HD09 KX24 LC15 LD19
5K067 AA30 BB21 DD11 DD17 EE02 HH23 HH36

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-023420**
(43)Date of publication of application : **24.01.2003**

(51)Int.Cl. **H04L 9/08**
G06F 13/00
G06F 15/00
G09C 1/00
H04L 12/56
H04Q 7/38

(21)Application number : **2002-069405**
(22)Date of filing : **14.03.2002**

(71)Applicant : **NEC CORP**
(72)Inventor : **REDLICH JENS-PETER**
KUEHNEL THOMAS
MUELLER WOLF

(30)Priority

Priority number	Priority date	Priority country
2001 278436	**26.03.2001**	**US**
2002 057914	**29.01.2002**	**US**

(54) COMMUNICATION METHOD THROUGH INTERMEDIARY OF UNTRUSTED ACCESS STATIONS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a mechanism that enables sharing of the existing infrastructure for accessing public or private IP networks, such as the public Internet or private LANs.
SOLUTION: The method of this invention includes the steps of establishing an connection between a terminal U and an untrusted access station A, transmitting a user authentication request to an internet service provider (ISP) P which is contracted with the terminal U, and establishing a trusted association between the terminal U and a trusted gateway T upon correct authentication of the ISP P and the terminal U. Through such an established secure tunnel, the ISP P can dynamically acquire control of resources by the access station A, in order to provide a prescribed service to the terminal U. After the legal authentication between the terminal U and the ISP P, the ISP P can generate a session key to encrypt data packets.